A METHOD AND APPARATUS FOR A COMMON-CAUSE
FAILURE MODULE FOR PROBABILISTIC RISK ASSESSMENT TOOLS

Inventors: Franciscus J. Groen

Carol S. Smidts

Ali Mosleh

BACKGROUND OF THE INVENTION

Field of the Invention

[0001]   The present invention generally relates to risk assessment tools used in risk modeling. More particularly, the present invention relates to the treatment of common cause failures in software tools for performing a probabilistic risk assessment (PRA).

Background Art

[0002]   Common-cause failure is a known concept within the risk assessment community and is defined as the simultaneous, dependent failure of multiple components in a system due to a shared cause. Common-cause failure models typically address these dependent failures by introducing into the risk models events known as common-cause basic events, which represent the dependent failure of two or more components. The set of common-cause basic events to be introduced into the risk model is derived from a specification of common-cause failure groups created by a risk analyst. Common-cause failure groups are groups of components that the risk analyst considers to be subject to shared causes of failure.

[0003]   One technique used in conventional risk modeling includes the use of PRA tools in which the risk model is scenario-based. Scenario-based modeling is accomplished using models known in the art as event sequence diagrams (ESDs). An ESD is a schematic representation of a sequence of events leading up to and contributing to a failure in the system being modeled. That is, the ESD is a flowchart with a number of paths showing an overall

view of the failure and a combination of components or occurrences leading to the failure. An ESD typically consists of a number of interrelated events. A first of these events is called an initiating event which represents the occurrence of an event significant enough to trigger a catastrophic failure in the modeled system.

[0004]   Also included in the ESDs are pivotal events, which are interim events whose occurrence or invocation may mitigate or aggravate the probability of occurrence of the initiating event. Finally, the ESD includes an end-state representative of a failure or success of the system due to the initiating event and the pivotal events. A complete ESD will include only one initiating event but may include many pivotal events and end states. The initiating event, the pivotal events, and the end-state are schematically related in a manner that will be discussed in greater detail below.

[0005]   The pivotal events may be further defined and examined within structures known as fault trees. Each fault tree represents one pivotal event. A fault tree is a schematic representation of the events that contribute to the occurrence of the pivotal event. Thus, an entire ESD may be expressed in terms of a number of different interrelated fault trees, each representing subcombinations of events that contribute to the corresponding pivotal event. The events that form the fault trees are low level events known as basic events. The makeup and structure of the fault trees will also be discussed in greater detail below.

[0006]   Typically, the basic events, which form the fault tree, may be modeled as independent events, meaning that the occurrence or nonoccurrence of each of the events in the ESD is assumed to be unaffected by the occurrence or nonoccurrence of the other basic events. In general, common-cause failure modeling is concerned with situations where multiple basic events are considered to occur due to a single cause. As stated above, a group of basic

events considered to be susceptible to a common-cause failure is known as a common-cause group.

[0007]   Existing failure models are structured to include and analyze ESDs and fault trees. However, the existing failure models are unable to accurately determine the probability that a common-group will contribute to a system failure. Also, the existing models are unable to efficiently quantify the extent to which the probability of the common cause group can be distributed to the common cause basic events within the group.

[0008]   In terms of common-cause failures, for example, traditional failure models are able to determine the significance of an independent basic event within the ESD. The process of determining whether regular basic events (independent) may also be members of a much more complex common-cause group is a time-consuming task and therefore more difficult. This process is typically manually accomplished by the individual risk analyst. In these failure models, although it is known that an individual basic event may also be a common-cause event, the model is unable to automatically determine and quantify the extent to which the basic event will likely contribute to the failure of the system under test.

[0009]   What is needed therefore is a common-cause failure module that is designed with an inherent awareness of the rules for constructing and quantifying common-cause groups and common-cause basic events, and then use these rules to aid the risk analyst in correctly and efficiently introducing these common-cause failures into the risk models.

BRIEF SUMMARY OF THE INVENTION

[0010]   According to an aspect of the invention, a common-cause failure module is provided which automates the insertion of common-cause basic events into multiple fault-tree structures. In case a regular basic event is found

10/09/01   SKGF Ref.: 1797.0510000

to be a member of a common-cause group, that basic event is automatically replaced by a logical operation that has two or more of the appropriate common-cause basic events associated with the common-cause group. Whenever an uncertainty analysis of the risk model is performed, the common-cause failure module correctly samples the probabilities for the common-cause basic events, such that dependencies and their probabilities are appropriately accounted for within the model.

[0011]   Consistent with the principles of the present invention as embodied and broadly described herein, the invention includes a computer-readable medium carrying one or more sequences of one or more instructions for execution by one or more processors. The instructions, when executed by the one or more processors, cause the one or more processors to perform the step of automatically inserting common-cause basic events into multiple tree structures in a risk model stored in a computer memory. The processors also perform the step of replacing regular basic events within the multiple tree structures with logic gates including two or more common-cause basic events associated with the common-cause failure group. The logic gates are based on a single definition of a common cause failure group.

[0012]   In another embodiment, the invention is directed to a method for enabling a user to identify common-cause failure groups within a software risk model stored on a machine-readable computer memory. The method comprises the steps of permitting a user to display a list of existing common-cause failure groups associated with the risk model via a graphical user interface and permitting the user to modify the list using the graphical user interface.

[0013]   In yet another embodiment, the invention is directed to a system including a processor and a memory comprising a first database stored in the memory, including data representative of a system risk model. The risk model includes at least one event system diagram and a number of fault tree

10/09/01   SKGF Ref.: 1797.0510000

definitions corresponding to the event system diagram. The fault tree definitions are adapted to model an influence of system component failures upon the system. Each fault tree relationship is formed of a number of inter-related basic events. The system also includes a common-cause group defining mechanism configured to permit a user to define a common-cause group in accordance with a number of inter-related basic events. The common-cause group defining mechanism includes one or more graphical user interfaces configured to display defined common-cause groups and permit the user to load the defined common-cause groups into the first database. The common-cause groups are defined in terms of common-cause basic events, each corresponding to a regular basic event. Also included in the system are a fault tree data structure mechanism and a common-cause failure expansion mechanism.

[0014]   The fault-tree data structure mechanism is configured to define a fault-tree data structure stored in the memory and adapted to convey an interdependence between the fault-tree definitions to form fault trees. The common-cause failure expansion mechanism is configured to apply common-cause failure expansion rules stored in the memory and adapted to convey a union of the regular basic events and the common-cause basic events. The processor is configured to apply the common-cause failure expansion rules to the fault trees to produce an expanded data structure representative of an occurrence of the common-cause basic events. Finally, the expanded data structure is displayed to the user via the one or more graphical user interfaces.

[0015]   Features and advantages of the invention include a risk module capable of aiding a risk analyst to recognize the probabilities associated with common-cause groups and common-cause basic events and their impact on the operation of the modeled system. Such a module can be implemented using a number of different approaches and will provide the analyst with a technique

that is more accurate, more efficient, and faster in understanding the probabilities associated with failure events.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016]   The accompanying drawings, which are incorporated herein and constitute a part of the specification, illustrate an embodiment of the invention and, together with the description, explain the purpose, advantages, and principles of the invention. In the drawings:

[0017]   FIG. 1 is a conventional event sequence diagram used in a risk model;

[0018]   FIG. 2 illustrates conventional fault trees associated with the event sequence diagram of FIG. 1;

[0019]   FIG. 3 is a block diagram representation of an exemplary system constructed and arranged in accordance with the present invention;

[0020]   FIG. 4 is an illustration of a hypothetical common-cause group based upon the fault trees shown in FIG. 2;

[0021]   FIG. 5 is an exemplary graphical representation of a risk analyst tool for defining a common-cause failure group;

[0022]   FIG. 6 is an exemplary graphical representation of a risk analyst tool for defining common-cause basic events in accordance with the representation of FIG. 5;

[0023]   FIG. 7 is an exemplary graphical representation of a risk analyst tool for selection of an expansion model associated with the analyst tool of FIG. 6;

[0024]   FIG. 8 is an exemplary embodiment of a risk analyst tool applying an uncertainty probability analysis;

[0025]   FIG. 9 is an exemplary representation of a risk analyst tool permitting a user to enter parameters associated with basic event probability determinations;

[0026]   FIG. 10 is an exemplary graphical representation of a fault tree including a top event and a number of regular basic events logically connected to form and produce the top event;

[0027]   FIG. 11 is a graphical representation of the fault tree shown in FIG. 10 expanded to show common-cause basic events; and

[0028]   FIG. 12 is an exemplary graphical representation of the fault tree shown in FIG. 11 using logic gates to replace the common-cause basic events.

DETAILED DESCRIPTION OF THE INVENTION

[0029]   The following detailed description of the present invention refers to the accompanying drawings that illustrate exemplary embodiments consistent with the invention. Other inventions are possible, and modifications may be made to the embodiments within the spirit and scope of the invention. Therefore, the following detailed description is not meant to limit the invention. Rather, the scope of the invention is defined by the appended claims.

[0030]   It would be apparent to one of skill in the art that the present invention, as described below, may be implemented in many different embodiments of hardware, software, firmware, and/or the entities illustrated in the figures. Any actual software code with specialized, controlled hardware to implement the present invention is not limiting of the present invention. Thus, the operation and behavior of the present invention will be described with the understanding that modifications and variations of the embodiments are possible, given the level of detail presented herein.

[0031]   Referring to the figures, FIG. 1 shows a traditional event sequence diagram (ESD) 102. In FIG. 1, the ESD 102 includes an initiating event 104. As stated above, an initiating event can be any event that creates a catastrophic failure or a significantly undesirable outcome in the system being modeled.

10/09/01   SKGF Ref.: 1797.0510000

The initiating event could be human-oriented, hardware-oriented, or could be introduced into the system through some external event. A meteor strike in an orbiting space shuttle, for example, can represent an initiating event.

[0032]   The initiating event 104 is serially connected to pivotal events 106, 108, and 110. The pivotal events are events that determine how and the extent to which the initiating event produces a desirable or undesirable end-state 112 in the system. End-states, such as the end-state 112, are defined by the risk analyst and are a measure of whether the pivotal events were mitigating factors or aggregating factors in the propagation of the initiating event 104 through the system. Each ESD includes one initiating event schematically connected to a number of pivotal events and end states.

[0033]   The initiating event 104 can represent a meteor strike and subsequent on-board fire. In the example of FIG. 1, the pivotal event 106 can represent whether an air crew member recognized that fragments from the meteor strike created a breach in the Shuttle's hull. The pivotal event 108 can represent whether the air crew member activated the proper procedures to respond to the breach. Finally, the pivotal event 110 might represent whether the fire was extinguished. The end-state 112 represents a satisfactory end result. The pivotal event 114 can represent, for example, whether the depressurizing system was used. The end-state 116 would represent a satisfactory conclusion to the pivotal event 114. An end-state 118 can represent a catastrophic failure of the space shuttle if the depressurizing system did not work properly.

[0034]   During operation, the analyst interprets the event sequence diagram 102 in the following manner: when the initiating event 104 occurs, then the pivotal events 106, 108 and 110, must also each occur. If they do occur, the successful end-state 112 is the result. If, however, the vents 106 and 108 occur but the event 110 does not occur and the pivotal event 114 occurs, then the successful end-state 116 will occur. If the pivotal event 114 did not occur, the failure would result. If the pivotal event 116 occurred but the pivotal event

108 did not occur, then a successful end-state 120 would occur. Finally, a pivotal event 122 can represent some other user interaction required only if the pivotal event 106 did not occur. If the pivotal event 122 occurred, the successful end-state 124 will occur. On the other hand, if the pivotal event 122 did not occur, a failure end-state 126 would occur.

[0035]   The pivotal events of an ESD may be expressed in terms of a fault tree, such as the fault trees shown in FIG. 2. A fault tree is a decision tree that is limited to binary outcomes for each of the pivotal events associated with an ESD. More specifically, FIG. 2 shows fault trees 200 and 201, which respectively correspond to the exemplary pivotal events 106 and 108 from the ESD 102. The fault tree is representative of a deductive reasoning process that determines what must happen in order for the pivotal event to occur. Traditional fault trees include a top event that represents occurrence of the corresponding pivotal event. A fault tree also includes a number of basic events that logically combine to spawn the occurrence of the top event.

[0036]   The basic events represent the lowest level of occurrence in the system that may contribute to the occurrence of their corresponding pivotal event. Fault trees use logical gates such as AND gates and/or OR gates to represent the relationships between the basic events and the top event within the fault tree. Within the scope of a risk model, basic events cannot be broken down into smaller contributing events. Additionally, each basic event possesses its own unique probability of occurrence that is independent from the occurrence of all of the other basic events. Thus, if the fault trees are properly constructed and analyzed, they will provide the risk analyst with an estimate of the likelihood of an occurrence of the top event of the fault tree based upon a probability of occurrence associated with the individual basic events.

[0037]   In FIG. 2, for example, the fault tree's top event and the pivotal event 106 will occur if the basic events 202, 204, and 206, each occurs, as shown by presence of an AND gate 208 connecting the basic events to the pivotal event

106. Similarly, the fault tree 201 shows that if basic events 206 and 208 occur, as represented by an AND gate 210, then the pivotal event 108 will also occur.

[0038]   It is also shown in FIG. 2 that the basic event 206 appears in each of the fault trees 200 and 201. The basic event 206 is therefore a common cause basic event. Thus, in FIG. 2, both of the pivotal events 106 and 108 depend on the occurrence of the basic event 206. That is, if the basic event 206 occurs in connection with the pivotal event 106, then it will already be present when the pivotal event 108 occurs. This relationship is referred to as a dependency between the occurrence of the pivotal events 106 and 108. Although the dependency between the pivotal events 106 and 108 can easily be recognized in the fault trees 200 and 201 of FIG. 2, most fault trees usually contain hundreds or thousands of basic events that must be manually identified in conventional PRA models. Therefore, the conventional PRA models sincerely limit the risk analyst's ability to quickly recognize the dependencies created by the common cause basic events. In the present invention however, the dependencies and common cause basic events can be automatically recognized, thereby aiding the risk analyst in correctly and efficiently introducing the impact of common cause failures into the risk models.

[0039]   FIG. 3 shows an exemplary common cause failure module 300 constructed and arranged in accordance with the present invention. In FIG. 3, the common cause failure module 300 includes a graphical user interface 302, a common cause group definer 304, a main computer 306, a fault tree structure module 308, a rule expansion module 310, and a system computer 312. Also included is a computer memory 314. The graphical user interface 302 can be implemented using any conventional display means, such as a computer monitor along with a keyboard or mouse, a touch screen display, or any other suitable alternative.

[0040]   The fault tree structure module 308 and the rule expansion module 310 are implemented in software in the present invention, although they could be implemented in hardware, firmware or any combination thereof. As stated above, the common cause failure module 300 assists the risk analyst in identifying common cause failures and determining the probability and the extent to which these common cause failures impact the occurrence of system components. The common cause group definer 304 is used by the risk analyst to identify and quantify common cause groups such as the exemplary common cause group 400, shown in FIG. 4.

[0041]   FIG. 4 shows the exemplary common cause group 400 that can result from fault tree dependencies, such as the dependency between the fault trees 200 and 201 shown in FIG. 2. In FIG. 4, the common cause group 400 includes the common cause basic event 206 from the fault trees 200 and 201. For purposes of illustration, an additional common cause basic event 402 can be included that may correspond to any of the other pivotal events 110, 114, and/or 122 of the ESD 102. FIG. 4 shows that the basic event 206 can occur in the fault trees 200 independently, as a regular basic event 206a, or dependently, as a common cause basic event 206b. Similarly, the basic event 402 can appear in its corresponding fault trees as an independent regular basic event 402a or dependently, as a common cause basic event 402b. In order to properly recognize the common cause group 400 using the present invention, a risk analyst will be presented with a number of graphical presentations via the graphical user interface 302, such as the screenshot shown in FIG. 5.

[0042]   Such a need can arise when the analyst needs to edit existing common cause groups or create new common cause groups due to changes in the operation of the components that combine to form the system being modeled. Additionally, the risk analyst might need to reorder the position of pivotal events within the ESD to reduce the impact of a failure likely to result from a catastrophic initiating event. Each of these scenarios presents the risk analyst

with a need to efficiently and quickly edit existing common cause groups or create new common cause groups within the risk model. Since previous versions of an analyst's model will likely include regular basic events, common cause basic events, and common cause groups, the first step the risk analyst must undertake to identify the common cause groups that already exist.

[0043] The screenshot 500 is provided to show the user all existing common cause groups within the risk model. Since the regular basic events and the common cause basic events are all associated with a particular ESD, the screenshot 500 presents the user with a particular ESD designator ID 502, identifying the associated ESD. Here, the designator ID corresponds to an identified common cause failure group 504 as shown. The user can also be presented with a number of options 506 pertaining to use of the screenshot 500, such as a common cause group filter. The user scrolls the exemplary screen 500 to find the existing common cause groups. The user is presented with additional screen shots after completing entries in the screen 500 to complete the process of defining new common cause groups.

[0044] Another exemplary screen, such as the screenshot 600, shown in FIG. 6 includes a reference to the common cause group created or edited in the analyst's previous session using the screenshot 500. For example, a designator 602 in the exemplary screen 600 associates the screen with the common cause group created in the screen 500. The screen 600 is also known as a common cause group instance. Here, the analyst is presented with a global list 604 of all of the basic events in the corresponding ESD. As discussed above, the risk analyst may desire to edit existing common cause groups or create new ones.

[0045] Thus, from within the global list 604 the risk analyst can select those basic events which are believed to be members of a common cause group and which the analyst desires to determine specific probabilities associated therewith. As shown, for example, the analyst can select a group of basic

events 606 to examine as a common cause group. Using the present invention, the analyst chooses the basic events 606 (events C and B) from the global list 604 and inserts those events into a member list 608 of common cause basic events.

[0046]   Each basic event must be a member event of at most one screen shot associated with a particular ESD to preclude ambiguous expansions. Expansions will be discussed in greater detail below. Having now defined the common cause group 606, the user can now determine the different probabilities associated with the group, as well as those associated with the individual events C and B. More specifically, the risk analyst can now determine the likelihood that the basic events C and B of the common cause group 606 will contribute to a failure as independent regular basic events or dependently, as common cause basic events.

[0047]   In practice, the common cause group can be any suitable data structure configured for storage in a computer memory, such as the memory 314 of the main computer 306.

[0048]   When a system under test is initially modeled, the associations that form the fault trees can also be stored in the memory 314. These fault tree definitions can include, for example, a definition of the top event in the fault tree and the identification of all the associated basic events. The fault tree definitions are stored in the memory 316 when the risk model is initially created.

[0049]   With the common cause group definitions defined and stored in the memory 314, the risk analyst can now select a common cause expansion model to apply the common cause group. The expansion model specifies rules for expanding regular basic events into common cause basic events and rules for quantifying the common cause basic events. The risk analyst also may use the model to describe the uncertainty about the total probability associated with the common cause group. The expansion is then used to update the

corresponding fault tree. Traditional models include the Alpha Factor and Beta Factor models, although others may be used. The expanded fault tree structure illustrates how probabilities associated with the common cause basic events relate to the associated pivotal events. Selection of the expansion model is accomplished using, for example, the exemplary screenshot 700, of FIG. 7.

[0050]   In FIG. 7, a window is shown on one side of the screenshot 700 and the available risk models are shown in another window. The particular risk model to be applied may be chosen from a number of conventional expansion models such as the global expansion (Beta Factor model) 702 and the full expansion (Alpha Factor model) 704.

[0051]   For purposes of illustration, the common cause basic event C of the common cause group 606 will be chosen as well as the exemplary full expansion model 704 from the screen 700. With the full expansion model 704 selected, the Alpha Factor rules, will be applied during the expansion process. An exemplary preview of a visualization of the expansion is shown in the screen area 706 of the exemplary screenshot 700.

[0052]   Here, the basic event C of the common cause group 606 is shown to be a regular basic event C(1). The event C is also shown as a common cause basic event CC3(2). That is, the basic event C may contribute to a system failure as a regular basic event or as a common cause basic event CC3(2). Thus, the window 706 gives the risk analyst a preview of the expansion of the common cause group that includes the basic event C. Next, the risk analyst must determine the probability of occurrence associated with the expanded common cause group.

[0053]   Referring back to FIG. 3, when the fault tree definitions have been completed, they are loaded into the fault tree structure module 308 to complete the construction of the fault tree. The module 308 associates the stored definitions with a data structure suitable for presentation via the graphical user

interface 302. The completed fault tree is then loaded into the rule expansion module 310.

[0054]   Similarly, when the common cause group definitions have been completed, the completed definitions are also loaded into the rule expansion module 310.   The received fault tree is then defined and expanded in accordance with the received common cause group definitions and the selected expansion rules.   The output of the rule expansion module is therefore a completed fault tree structure showing not only the associated regular basic events, but also the common cause basic events that create the dependencies between different fault trees. The final expanded tree is then presented to the user via a graphical representation that can be more carefully examined and analyzed.   In practice, the fault tree structure module 308 and the rule expansion module 310 can be a dedicated computer processor, although the present invention is not limited to such an implementation.

[0055]   The risk analyst can now quantify the uncertainty about the total probability of the selected common cause group.   An exemplary screenshot, such as a screenshot 800, is presented to the user as a first step in this process. Specifically, in an exemplary embodiment of the common cause failure module, the analyst is permitted, via the exemplary screenshot 800, to determine the total probability of occurrence of the common cause failure group. However, since uncertainty surrounds determination of any probability assessment, the total probability of the common cause basic event may be more accurately expressed in terms of the uncertainty about the total probability.

[0056]   The exemplary screenshot 800, permits the risk analyst to express the uncertainty about the total probability of the common cause failure group. The total probability (Q_T) may be graphically represented by a number of standard distribution curves, such as a beta, gamma, or other suitable distribution curves. Stated another way, when the fault tree is constructed

containing the regular basic event C(1) and the common cause basic CC3(2) as shown in FIG. 7, the user may apply the expansion model rules to quantify Q_T. In so doing, the user can more accurately determine the uncertainty that the regular basic event C(1) and the common cause basic event CC3(2) will contribute to a system failure.

[0057]   Concerning probabilities associated with regular basic events in general, risk modelers, through experimentation and analysis, have developed uncertainty factors that may be associated with the components of any system within the risk model. That is, the uncertainty factors are already known and may be simply entered into the common cause failure module by the risk analyst in order to plot the uncertainty about Q_T.

[0058]   Each of the basic events shown in the global list 604 of FIG. 6, as a regular basic event, is associated with a static probability of occurrence determined through experimentation, derivation, and analysis as discussed above. Using the screenshot 800 of FIG. 8, the risk analyst can express Q_T in terms of a preferred distribution curve such as the gamma curve. In FIG. 8, a graph 808 is a gamma distribution plot and is used to illustrate the uncertainty surrounding Q_T of the regular basic events without any association with the common cause groups. This is accomplished with the risk analyst specifying parameters required in the screen 800, such as the distribution for the total probability 801, a mode of input 802, a specific scale factor 804, and a shape 806.   Thus, Q_T without any association with common cause factors is expressed in the graph 808 of the screenshot 800.

[0059]   More specifically, an analyst can determine that if starting with Q_T of an event as a regular basic event using parameters 810 and 812, then these parameters and additional parameters may be taken together to further determine the total probability of the same events as members of a common cause group. Thus, as stated above, the user may select a distribution for Q_T

from among the available techniques Each technique is a mathematical function expressed in terms of parameters that can be selected by the analyst.

[0060]   In the graph 808, the user specifies parameters 810 along the vertical access and parameters 812 along the horizontal access of the plot. The parameters 810 may be specified, for example, in terms of a cumulative density function (CDF) or probability density function (PDF), etc. Thus the uncertainty plot 808 for Q_T can be interpreted as indicating that there is a 50% chance that the actual value of the probability of the common cause group containing the basic events C(1) and CC3(2) is smaller than about .0015. Similarly, as can also be observed from the graph 808, there is about a 75% chance that the value of this probability will be smaller than about .004.

[0061]   Next, with the risk analyst having determined that the uncertainty about Q_T for the common cause group, a determination must now be made as to how Q_T can be distributed across the individual members of the common cause group, the regular basic event C(1) and the common cause basic event CC3(2). The extension of Q_T to the common cause group can be extended to the probability for the individual basic events using, for example, a Beta Factor model and using the following expression:

[0062] $Q_I = (1-\beta) * Q_T$; and   (1)

$Q_{CC} = \beta * Q_T$ (2)

[0063]   Where Q_I is the probability of common cause basic events representing independent failures, and Q_{CC} is the probability of the common cause basic events representing dependent failures, the analyst specifies the uncertainty about Q_I and Q_{CC} in terms of uncertainty distributions about Q_{CC} and β. The above equations define a correlation between Q_I and Q_{CC} for the Beta Factor model.

[0064]   FIG. 9 presents an exemplary screenshot 900 providing the risk analyst with a tool which provides the capability to enter all of the parameters associated with the expansion model. In FIG. 9, the screenshot 100 includes a

full expansion, as specified by the full expansion using, by way of illustration, the Alpha Factor model 704 shown in FIG. 7. By expanding the common cause group, including the regular basic event C(1) and the common cause basic event CC3(2), in terms of a full expansion, the Alpha Factor model is applied in order to distribute the total probability across each of the basic events. Here, the risk analyst selects a first alpha factor 902 and a second alpha factor 903 for use as initial values associated with the model. The alpha factors 902 and 903 are analogous to the value β used in equations one and two above and applicable to the Beta Factor model. Here, however, since the risk analyst has chosen the full expansion in accordance with the Alpha Factor model 704, alpha factors must be selected instead of beta factors. Thus, using the Alpha Factor model, the risk analyst must specify one or more alpha factor parameters in order to distribute the total probability Q_T of the common cause group across the basic events C(1) and CC3(2).

[0065]   The values for the alpha factor 902 and the alpha factor 903 are also chosen in uncertain terms as are the values for β and Q_T from equations (1) and (2) above. Since the exact value for the alpha factor 902 and the alpha factor 903 are not precisely known, they must be specified or selected in terms of uncertainty. As noted above, the uncertainty on the total probability Q_T was expressed in the plot 808 in terms of a gamma distribution. A gamma, log normal, or other type distribution could be used for the screen 900. However, the inventors of the present invention have chosen to express the uncertainty as determined by the Alpha Factor model, in terms of a beta distribution. The selected alpha 1 factor 902 and the alpha 2 factor 903 parameters determine the way in which Q_T will be distributed about the common cause basic events. Next, a parameter A (904) and a parameter B (906) must be chosen by the analyst for each of the alpha factors 902 and 903 in accordance with the selected beta distribution.

[0066]   Parameters A (904) and B (906) can be selected based upon experimentation analysis and a general knowledge of the probability that certain components of the system under test may or may not fail. Also, as known in the art, parameters A (904) and B (906) may be selected based upon defined default values that are conventionally characteristic of beta distributions. Here, for purposes of illustration, the values for parameters A and B have been chosen as 2.1 and .4 respectively which in turn are used to specify the uncertainty about alpha factor 1 for applying a beta distribution. The parameters A (904) and B (906) in the exemplary screen 900 are analogous to the parameters 804 and 806 associated with the exemplary screen 800 in FIG. 8, in that they are selected by the risk analyst and are chosen based upon archived experimental and/or analytical data. Similarly, for the alpha 2 factor 903 in the exemplary screen 900, parameter A has been chosen to be .03.

[0067]   Therefore, what is implied by the risk analyst selecting the noted values for the alpha factors 902 and 903 and the parameters A (904) and B (906) is a best estimate by the analyst. The estimate suggests that based upon all of the selected parameters, the mean value associated with the beta distribution is about 8.4×10^{-1} with the 5th percentile being about 4.05×10^{-1} and the 95th percentile being about $9.9 \times 10\text{-}1$. The 5th percentile can be viewed as a lower bound estimate while the 95th percentile can be viewed as an upper bound estimate for alpha 1 factor 902. If the risk analysts were to change the parameter A (904) and/or parameter B (906) for alpha 1, the mean value, the 5th percentile, and the 95th percentile values 908, 910 and 912, would all change.

[0068]   As discussed above, the particular values for parameters A and B may be chosen through extensive life cycle testing regarding failures of system components, experimentation, and hypotheticals regarding mean time between

failure associated with system components. In the present invention, however, the risk analyst chooses these values.

[0069] For example, in the case of the space shuttle, the noted parameter values can be derived from tables which result from an analysis to determine how likely is it that if any of the engines failed or any of the power supply systems failed, it will trigger the failure of other engines or other power supply systems. The exemplary screen 900 merely conveys an interdependence of the various probabilities as distributed between regular basic events and common cause basic events associated with particular fault trees. A window 914 in the exemplary screen 900 is used by the analyst to specify the desired number of events to be included in the analysis, the number of simultaneous events or any other factors or variations that may be desirable in terms of performing a common cause probability analysis.

[0070] Again, referring back to FIG. 3, now that the risk analyst has entered all of the appropriate data into the expansion models, the rule expansion module 310 can apply this data to expand the fault tree to present a visualization to the risk analyst via the graphical user interface 302.

[0071] FIG. 10 presents an exemplary screen 1000 showing the fault tree and indicating of the logical relationships shared between the associated basic events. In FIG. 10, an exemplary screenshot 1000 shows a fault tree 1001 including a top event 1002, a logic gate 1004, a logic gate 1006 and a logic gate 1008. Also shown is a list of exemplary basic events 1010, 1012, 1014, and 1016. As represented in the fault tree, the logic gate 1006, here chosen as a logical OR gate, connects the basic events 1010 and 1012. The logic gate 1008 is a logical AND gate and logically connects the basic events 1014 and 1016. The screenshot 1000 is presented as a view of the fault tree before application of the expansion rules to be applied by the rule expansion module 310 shown in FIG. 3. After application of all of the expansion rules, the

common cause dependencies can now be properly introduced into the fault tree structure. FIG. 11 illustrates this introduction.

[0072]   FIG. 11 presents an exemplary screen view 1100 showing an expanded version of the fault tree 1001. It will be noted that in the fault tree 1101 shown in FIG. 11, the basic event 1010 which was shown in FIG. 10 as an independent event is now graphically indicated to have been expanded according to the logic of the common cause group 1102. Similarly, the basic event 1014 as shown in association with basic event C is now shown to be a member of a common cause group, and has therefore been expanded 1104.

[0073]   Thus, common cause group 1104 illustrates that one basic event can exist as a regular basic event 1014 and a common cause basic event 1114, which represent the potential for an independent failure or a dependent failure attributed to the same event. The basic events 1012 and 1016 remain unchanged in this particular fault tree structure, since they do not belong to a common cause group. As noted in FIG. 11, the common cause groups 1102 and 1104 are represented by a double circle configuration. Also noted in FIG. 11, a probability mean value 1116 associated with the occurrence of the common cause group 1102 can also be indicated as shown in window 1118. Any other data determined desirable by the analyst, can be similarly displayed. Since the double circle configuration can be difficult to view, the risk analyst is provided with an extended expansion tool to graphically distinguish between the common cause basic events and the regular basic events.

[0074]   FIG. 12 presents an extended expansion view showing the expansion of regular basic events 1010 and 1014 into common cause basic events 1210 and 1214, and 1216, common cause basic event 1216 being common to the expansion of basic event 1010 as well as basic event 1014. FIG. 12 also shows the automatic replacement of the basic events by a logical operation showing the common cause basic events associated with the common cause group. As shown in FIG. 12 the common cause basic event 1102, previously

shown in FIG. 11, has been replaced with a logical OR gate 1202 to more clearly illustrate the relationship between the basic events and the top event in the fault trees, and to provide more detail about the exact nature of the expansion of basic events.

[0075]   In FIG. 11 the top event 1002 is shown to occur if the common cause basic event 1102 occurs or basic event 1012 occurs in combination with an occurrence of the common cause basic event 1104 and an occurrence of the regular basic event 1016.

[0076]   In FIG. 12 however, it can be seen that the common cause basic event 1102 has been replaced with an OR gate 1202 indicating that the basic event that formed the common cause group 1102 can exist as the independent event 1210 or as the common cause basic event 1216. This means that one basic event can contribute to a failure as an independent event or as a dependent event, each having its own probability of occurrence.

[0077]   Similarly, the common cause basic event 1104 shown in FIG. 11 is replaced with the OR gate 1204 shown in FIG. 12, indicating that the basic event that formed the common cause group 1104 can create a failure as regular independent basic event 1214 or as the common cause dependent basic event 1216. Event 1216 is common to the expansion of group 1102 and 1102, introducing the dependence between the events into the risk model.

[0078]   Such an expanded fault tree visualization, as discussed in relation to the present invention, aids the risk analysis in quickly and efficiently determining which basic events are most likely to contribute to a system failure after reprioritizing pivotal events within an events sequence diagram.

[0079]   Thus, the present invention provides a common-cause failure module that is aware of the rules for constructing and quantifying common-cause failure groups and common cause basic events. The present invention is therefore capable of assisting the risk analyst in introducing common-cause

dependencies into the risk model and assessing their impact on system failures.

While the above description contains many specific features of the invention, these should not be construed as limitations on the scope of the invention, but rather as exemplary embodiments thereof. Many other variations are possible. Accordingly, the scope of the invention should be determined not by the embodiments illustrated, but by the appended claims and their legal equivalents.